

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出 願 年 月 日
Date of Application:

2000年 6月30日

願 番 号
Application Number:

特願2000-199266

願 人
Applicant(s):

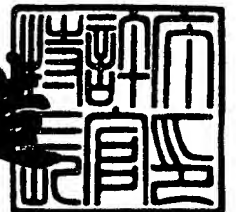
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年10月27日.

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3088499

【書類名】 特許願

【整理番号】 0051232

【提出日】 平成12年 6月30日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 G06F 11/36

【発明の名称】 L S I , L S I を搭載した電子装置、デバッグ方法、 L S I のデバッグ装置

【請求項の数】 13

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 川崎 雄介

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 橋本 繁

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100094514

【弁理士】

【氏名又は名称】 林 恒▲徳▼

【代理人】

【識別番号】 100094525

【弁理士】

【氏名又は名称】 土井 健二

【手数料の表示】

【予納台帳番号】 030708

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704944

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 L S I, L S I を搭載した電子装置、デバッグ方法、L S I のデバッグ装置

【特許請求の範囲】

【請求項 1】 内部回路と、

外部から前記内部回路をデバッグするためのデバッグ I / F 回路と、

前記デバッグ I / F 回路とデバッグ端子との間に設けられ、前記デバッグ I / F 回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と前記送信鍵とから認証を行い、前記デバッグ I / F 回路の動作を許可する認証回路とを有することを

特徴とする L S I。

【請求項 2】 前記認証回路は、前記動作の許可のため、前記デバッグ I / F 回路へのリセット信号を解除することを

特徴とする請求項 1 の L S I。

【請求項 3】 前記認証回路は、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合することを

特徴とする請求項 1 の L S I。

【請求項 4】 前記認証回路は、前記動作許可の時間待ちを行うことを

特徴とする請求項 1 の L S I。

【請求項 5】 前記認証回路は、前記送信鍵を乱数により生成することを

特徴とする請求項 1 の L S I。

【請求項 6】 内部回路と、外部から前記内部回路をデバッグするためのデバッグ I / F 回路と、前記デバッグ I / F 回路とデバッグ端子との間に設けられ、前記デバッグ I / F 回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグ I / F 回路の動作を許可する認証回路とを有する L S I を搭載したことを

特徴とする電子装置。

【請求項 7】 デバッグ I / F 回路を利用して、外部から内部回路をデバッグするデバッグ方法において、

前記デバッグ I / F 回路の起動時に、前記外部に送信鍵を送信するステップと

前記外部から受信した信号と前記送信鍵とから認証を行い、前記デバッグ I / F 回路の動作を許可するステップとを有することを
特徴とするデバッグ方法。

【請求項 8】前記認証ステップは、前記動作の許可のため、前記デバッグ I / F 回路へのリセット信号を解除するステップを有することを
特徴とする請求項 7 のデバッグ方法。

【請求項 9】前記認証ステップは、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合するステップを有することを
特徴とする請求項 7 のデバッグ方法。

【請求項 10】前記認証ステップは、前記動作許可の時間待ちを行うステップを有することを
特徴とする請求項 7 のデバッグ方法。

【請求項 11】前記送信ステップは、前記送信鍵を乱数により生成するステップを有することを
特徴とする請求項 7 のデバッグ方法。

【請求項 12】デバッグ装置と前記デバッグ I / F 回路の間に設けられた識別装置が、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信するステップを、更に有することを
特徴とする請求項 7 のデバッグ方法。

【請求項 13】内部回路と、外部から前記内部回路をデバッグするためのデバッグ I / F 回路と、前記デバッグ I / F 回路とデバッグ端子との間に設けられ、前記デバッグ I / F 回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグ I / F 回路の動作を許可する認証回路とを有する L S I をデバッグするデバッグ装置であって、デバッグユニットと前記デバッグ I / F 回路の間に設けられ、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信する識別装置を有することを

特徴とするデバッグ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、LSIの内部回路の挙動の不正取得を防止するためのセキュリティ機能を有するLSI、電子装置、LSIのデバッグ方法、電子装置のデバッグ方法及びデバッグ装置に関する。

【0002】

電子商取引等あらゆる分野で、よりセキュリティの高い装置が求められている。このため、あらゆる方法で装置の逆解析（リバースエンジニアリング）を防ぐ方法が考案されてきた。しかし、これらの試みにもかかわらず、裏ROM等が作成され、装置の開発者の不本意な用途に悪用される事が絶えない。このため、装置の動作そのものが、第三者に解析不能なシステムが求められている。

【0003】

【従来の技術】

図9は、従来技術の説明図である。図9に示すように、LSI110には、CPU200と周辺回路300と、これらを接続するバス600とが設けられている。このLSI110では、CPU200が、周辺回路300からデータ、プログラムを取得し、データ処理して、データを周辺回路300に出力する。

【0004】

一方、このLSI110を使用して、装置を開発する場合には、CPU200の処理状況を、直接モニタし、プログラム等の検証を行う。周辺回路300の出力データをモニタする検証方法も行われるが、出力に到るCPU200の挙動は、出力データからは解明できない。

【0005】

このため、CPU200に別のバス500を介しデバッグI/F（インタフェース）回路400が設けられている。LSI110外部のデバッグコントローラ100は、このデバッグI/F400に接続し、クロックCLKを供給し、信号SINを入力し、出力SOUTを得る。

【 0 0 0 6 】

このデバッグ I / F 回路 4 0 0 は、装置の開発時に、CPU 2 0 0 の挙動（プログラムカウンタ、レジスタ等の内容）を取得するのに、利用され、装置がフィールドに出荷された場合には、障害発生時、装置の診断時に、同様に利用される。

【 0 0 0 7 】

このような、デバッグ I / F 4 0 0 からのアクセスに対しては、従来は、セキュリティ機能を設けていない。

【 0 0 0 8 】

【発明が解決しようとする課題】

従来の通常のセキュリティを要しない装置では、デバッグ I / F 端子は未使用時／使用時にかかわらず、外部から見えており第三者による利用に対して全く無防備である。このため、フィールドへ出荷された装置場合には、第三者がデバッグ I / F 端子を用いる事で、中央処理装置（CPU）の挙動を正確に逆解析する事が容易にでき、セキュリティー上無防備であるという問題がある。

【 0 0 0 9 】

従って、従来の装置では、デバッグ I / F 機能を設けた CPU を装置が用いている場合には、第三者に分析の手がかりを与える事になる。例えば、デバッグ I / F 機能付きの CPU を用いた POS レジスタの場合には、デバッグ I / F のデバッグユニットとパソコン等を接続する事で、パスワードや暗号鍵等のデータですら容易に探し出す事が可能である。

【 0 0 1 0 】

従って、本発明の目的は、デバッグ I / F の利用を制限して、第三者の不正な逆解析を防止するための L S I ， 電子装置、デバッグ方法及びデバッグ装置を提供するにある。

【 0 0 1 1 】

本発明の他の目的は、L S I 内のデバッグ I / F 回路と外部端子との間に認証ロジックを設け、デバッグ I / F の利用に制限を設けるための L S I ， 電子装置、デバッグ方法及びデバッグ装置を提供するにある。

【 0 0 1 2 】

更に、本発明の他の目的は、L S I 内のデバッグ I / F 回路と外部端子との間に認証ロジックを解析することを防止するための L S I、電子装置、デバッグ方法及びデバッグ装置を提供することにある。

【 0 0 1 3 】

更に、本発明の他の目的は、デバッグ I / F の利用を制限した第 3 者の不正な逆解析を、検出するための L S I、電子装置、デバッグ方法、デバッグ方法及びデバッグ装置を提供することにある。

【 0 0 1 4 】

【課題を解決するための手段】

この目的の達成のため、本発明の L S I は、内部回路と、外部から前記内部回路をデバッグするためのデバッグ I / F 回路と、前記デバッグ I / F 回路とデバッグ端子との間に設けられ、前記デバッグ I / F 回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と前記送信鍵とから認証を行い、前記デバッグ I / F 回路の動作を許可する認証回路とを有する。

【 0 0 1 5 】

本発明の電子装置は、内部回路と、外部から前記内部回路をデバッグするためのデバッグ I / F 回路と、前記デバッグ I / F 回路とデバッグ端子との間に設けられ、前記デバッグ I / F 回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグ I / F 回路の動作を許可する認証回路とを有する L S I を搭載された。

【 0 0 1 6 】

本発明のデバッグ方法は、デバッグ I / F 回路の起動時に、前記外部に送信鍵を送信するステップと、前記外部から受信した信号と前記送信鍵とから認証を行い、前記デバッグ I / F 回路の動作を許可するステップとを有する。

【 0 0 1 7 】

本発明のデバッグ装置は、内部回路と、外部から前記内部回路をデバッグするためのデバッグ I / F 回路と、前記デバッグ I / F 回路とデバッグ端子との間に

設けられ、前記デバッグ I / F 回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグ I / F 回路の動作を許可する認証回路とを有する L S I をデバッグするデバッグ装置であって、デバッグユニットと前記デバッグ I / F 回路の間に設けられ、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信する識別装置を有する。

【0018】

デバッグ I / F 回路とデバッグ端子の間に認証回路を設けたため、第 3 者のデバッグ I / F を利用して、内部回路の動きをリバースエンジニアリングする等の不正行為から内部回路を守る事ができ、従来の装置よりもより高いセキュリティを保つ事ができる。

【0019】

又、識別装置 3 と L S I 2 とのセットでセキュリティを実現するため、物理的接続と認証アルゴリズムにより、セキュリティを行うため、高いセキュリティが可能となる。また、P C 5 による不正解析も困難である。

【0020】

又、本発明のデバッグ方法では、前記認証ステップは、前記動作の許可のため、前記デバッグ I / F 回路へのリセット信号を解除するステップを有する。本発明の L S I では、前記認証回路は、前記動作の許可のため、前記デバッグ I / F 回路へのリセット信号を解除する。このため、認証しても、既存のリセットの解除により、実現できる。

【0021】

更に、本発明の L S I では、前記認証回路は、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合する。本発明のデバッグ方法では、前記認証ステップは、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合するステップを有する。暗号化するため、より高いセキュリティが可能となる。

【0022】

本発明の L S I では、前記認証回路は、前記動作許可の時間待ちを行う。本発

明のデバッグ方法では、前記認証ステップは、前記動作許可の時間待ちを行うステップを有する。シリアルデータ鍵の判定前後に、タイマーを用いて、一致判定終了後の時間待ちをする。このため、第3者が、何らかの暗号鍵データを入力しても、認証結果（リセット）を得るまで時間がかかる。これにより、第3者による不正なデバッグI/F利用を防ぎ、また何度もリトライする際に莫大な時間がかかる。

【 0 0 2 3 】

本発明のLSIでは、前記認証回路は、前記送信鍵を乱数により生成することにより、送信するシリアルデータ（送信鍵）を起動の毎に、乱数をベースにすることで、毎回異なる送受信データとして、解析を困難としている。

【 0 0 2 4 】

【発明の実施の形態】

以下、本発明を、LSI、電子装置、他の実施の形態に分けて、説明する。

【 0 0 2 5 】

〔 L S I 〕

図1は、本発明の一実施の形態のLSI及びデバッグ機構のブロック図であり、図2は、その認証処理の説明図、図3は、正当使用時の動作説明図、図4は、不正使用時の動作説明図である。

【 0 0 2 6 】

図1において、2はCPU付きシステムLSIであり、本発明によるデバッグI/F利用認証回路が設けられている。1はLSI2内部のデバッグI/Fを利用するための外部デバッグコントローラである。3は識別装置であり、LSI2とデバッグコントローラ1の間に挿入して用いられ、LSI2内部の認証回路と連動し、認証を行う。

【 0 0 2 7 】

LSI2は、デバッグI/F回路2-1と、CPU2-2と、I/F回路2-1とCPU2-2を接続するデバッグバス4-1と、CPUバス4-2に接続された周辺回路2-12とを有する。周辺回路2-12は、LSIの用途により異なるが、例えば、図6以下で説明する電子マネー決済用回路である。

【 0 0 2 8 】

本発明の実施の形態では、このCPUバス4-2に認証回路が設けられている。認証回路の構成を説明する。

【 0 0 2 9 】

ポート4-2は、バス4-2からCPU2-2の書き込みデータを受ける。レジスタ2-5は、CPU2-2の生成したデバッグI/F利用送信鍵を格納する。レジスタ2-8は、CPU2-2の生成した認証鍵を格納する。送信回路2-4は、識別装置3によって供給されているクロックに同期してレジスタ2-5の送信鍵を送信する。シフトレジスタ2-6は、識別装置2からの返送された暗号鍵を受信する。

【 0 0 3 0 】

一致検出回路2-9は、シフトレジスタ2-6の暗号鍵とレジスタ2-8の認証鍵と比較して、一致を検出する。タイマー回路2-7は、一致検出回路2-9の一致検出出力に応じて、クロックの計数を開始し、一定時間後、内部のデバッグI/F回路2-1へのリセット信号を解除する信号を生成する。リセットゲート2-11は、リセット解除信号により、リセット信号のデバッグI/F回路2-1への入力を解除する。受信許可ゲート2-10は、送信回路2-4からの受信許可信号に応じて、信号入力端子SINからのデータを取り込むシフトレジスタ2-6をイネーブルにする。

【 0 0 3 1 】

次に、識別装置3には、鍵送受信回路3-1が設けられている。鍵送受信回路3-1は、識別装置3の電源が投入された時に、クロックを送信し、前述の送信鍵を受信して、あらかじめ決めておいたキーで暗号化して、暗号鍵を送信する。

【 0 0 3 2 】

次に、デバッグI/Fが利用可能となる動作手順を図1、図2により説明する。図1に示すように、デバッグI/Fを利用するデバッグコントローラ1を、識別装置3を介しLSI2に接続する。

【 0 0 3 3 】

①まず、LSI2と識別装置3の電源を投入し起動する。すると、識別装置3

よりLSI 2のデバッグI/F 2-1へクロックが供給される。同時にLSI 2内では、CPU 2-2が起動し、ファームウェアによりデバッグI/F利用送信鍵と認証鍵を生成し、バス4-2、ポート2-3を介しレジスタ2-5、2-8に書き込む。この時、送信鍵は乱数をベースに生成し、認証鍵は送信鍵をあらかじめ決めておいたキーを用いて暗号化して生成する。

【0034】

②鍵が書き込まれると、識別装置3によって供給されているクロックに同期して、送信回路2-4が送信鍵を送信する。

【0035】

③送信鍵を識別装置3内の鍵送受信回路3-1が受信して、あらかじめ決めておいたキーで暗号化して、暗号鍵を送信する。この時のキーは、先程LSI 2内のファームウェアによって用いたキーと同一のものである。

【0036】

④LSI 2では、返送された暗号鍵をシフトレジスタ2-6にて受信し、一致検出回路2-9にて、レジスタ2-8の認証鍵と比較して、一致していた場合のみ、タイマー回路2-7へ一致検出を伝える。タイマー回路2-7では、一定時間待ってから、ゲート2-11による内部のデバッグI/F 2-1へのリセット信号を解除する。

【0037】

こうして初めて、LSI 2のデバッグI/F回路2-1が利用可能となる。即ち、デバッグコントローラ1からリセット信号をLSI 2に送信し、デバッグI/F回路2-1をリセットし、デバッグI/F回路2-1を利用して、CPU 2-2にアクセスできる。

【0038】

図3に示すように、LSI提供メーカーは、装置開発メーカーに、LSI 2と識別装置3とを提供する。LSI 2の暗号化キーと、識別装置3の暗号化キーとは、同一のものである。装置開発メーカーは、LSI 2をターゲットボード7に搭載し、装置の開発を行う。

【0039】

デバッグを行う場合には、L S I 2 に識別装置 3 を接続し、識別装置 3 にデバッグコントローラ 1、P C インタフェイスボード 6、パーソナルコンピュータ 5 を接続する。識別装置 3 を間に入れると、前述の認証シーケンスが働き、リセットが解除されることで、P C 5 上のデバッガーが、デバッグ I / F 回路 2 - 1 を利用できるようになる。又、装置をフィールドに出荷した後も、識別装置 3 を接続することにより、P C 5 上のデバッガーが利用できるようになる。

【 0 0 4 0 】

一方、図 4 に示すように、識別装置 3 をつながない場合には、L S I 2 のデバッグ I / F 回路 2 - 1 はリセットを解除されず、P C 5 のデバッガーは、L S I 2 の C P U 2 - 2 をアクセス出来ない。例えば、装置のフィールドへの出荷後、第 3 者のデバッグ I / F を利用して、C P U 2 - 2 内部の動きをリバースエンジニアリングする等の不正行為から C P U 2 - 2 を守る事ができ、従来の装置よりもより高いセキュリティを保つ事ができる。

【 0 0 4 1 】

即ち、従来のパスワードの認証等のセキュリティ手法では、パスワードが漏れると、機能を発揮しなし、リトライにより、パスワードを解明しやすい。従って、多数のユーザーに提供される L S I 2 のセキュリティ機構として、不向きである。この実施の形態では、識別装置 3 と L S I 2 とのセットでセキュリティを実現するため、物理的接続と認証アルゴリズムにより、セキュリティを行うため、高いセキュリティが可能となる。また、P C 5 による不正解析も困難である。

【 0 0 4 2 】

又、前述の利用認証機能は、暗号化アルゴリズムのため、巧妙な不正者は、認証機構の存在を知り、暗号化鍵（データ）のリトライにより解析を試みる場合がある。この実施の形態では、この解析を困難にするため、次の手法を採用している。

【 0 0 4 3 】

第 1 に、シリアルデータ鍵の判定後に、タイマー 2 - 7 を用いて、一致判定終了後の時間待ちをする。このため、第 3 者が、図 4 の接続で、何らかの暗号鍵データを入力しても、認証結果（リセット）を得るまで時間がかかる。これにより

、第3者による不正なデバッグI/F利用を防ぎ、また何度もリトライする際に莫大な時間がかかる。

【0044】

第2に、送信するシリアルデータ（送信鍵）を起動の毎に、乱数をベースにすることで、毎回異なる送受信データとして、解析を困難としている。

【0045】

第3に、シフトレジスタの受信動作を、送信鍵の送信後、一定時間とし、1回の起動時に、1回の受信しかしないようにし、繰り返しデータを入力しても受け付けないため、解析を困難としている。

【0046】

次に、図5により、本発明の他の実施の形態の認証処理を説明する。

【0047】

①まず、LSI2と識別装置3の電源を投入し起動すると、識別装置3よりLSI2のデバッグI/F2-1へクロックが供給される。同時にLSI2内では、CPU2-2が起動し、前述のように、ファームウェアによりデバッグI/F利用送信鍵と認証鍵を生成し、バス4-2、ポート2-3を介しレジスタ2-5、2-8に書き込む。

【0048】

②鍵が書き込まれると、識別装置3によって供給されているクロックに同期して、送信回路2-4が送信鍵を送信する。

【0049】

③送信鍵を識別装置3内の鍵送受信回路3-1が受信して、あらかじめ決めたおいたキーで暗号化して、暗号鍵を送信する。この時のキーは、先程LSI2内のファームウェアによって用いたキーと同一のものである。識別装置3では、暗号鍵にユーザーIDを付加し、LSI2に送信する。

【0050】

④LSI2では、返送された暗号鍵をシフトレジスタ2-6にて受信し、一致検出回路2-9にて、レジスタ2-8の認証鍵と比較して、一致していた場合のみ、タイマー回路2-7へ一致検出を伝える。タイマー回路2-7では、一定時

間待ってから、ゲート 2-11 の内部のデバッグ I/F 2-1 へのリセット信号の入力を解除する。又、ユーザー ID は、ログされる。このため、万一、送信鍵の情報が漏れた際に、ログされたユーザー ID から、どのユーザーから漏れたかを特定できる。

【0051】

この実施の形態において、識別装置 3 で、受信した送信鍵とユーザー ID とをキーで暗号化する方法を採用することにより、ユーザー ID が容易に変更されることを防止できる。

〔電子装置〕

次に、前述のシステム LSI 2 を搭載した電子装置を説明する。図 6 は、システム LSI 2 の適用例の説明図であり、図 7 は、この適用例での LSI 2 の周辺回路の構成図、図 8 は、電子装置の説明図である。

【0052】

図 6 に示すものでは、システム LSI 2 は、カード決済用 LSI であり、デビットカード決済機能 40、クレジットカード決済機能 41、電子マネー決済機能 42、その他のサービス機能 43 を有する。このため、LSI 2 には、IC カードリーダー/ライター 30 と、磁気カードリーダー 31 と、表示及びキー 32 とが接続される。又、必要に応じて、レシートプリンタ 33 が接続される。これらの決済機能 40～43 は、LSI 2 の CPU 2-2 のプログラムの実行により、実現される。

【0053】

従って、この LSI 2 を搭載することにより、各種の電子装置 50～57 に、カード決済機能を付与できる。これらの電子装置は、例えば、POS 用リーダー/ライター 50、統合端末 51、モバイル端末 52、ATM（自動テラマシ）53、自動販売機 54、PDA（パーソナル機器）55、携帯電話 56、PC（パーソナルコンピュータ）57 である。

【0054】

このカード決済のための LSI 2 の周辺回路 2-12 を、図 7 により、説明する。周辺回路 2-12 は、スマートカードコントローラ 60 と、MS 制御回路 6

1と、LCD制御回路62と、マトリクスKB制御回路63と、メモリコントローラ64と、シリアル入出力ポート69～72とを有する。図7では、前述のLSI2は、ターゲットボード7に搭載された状態を示し、LSI2を説明の簡単のため、CPU2-2と周辺回路2-12（60-64、69-72）のみ示してある。勿論、デバッグI/F2-1、認証回路を有する。

【0055】

スマートカードコントローラ60は、ICカードリーダー/ライタ30を介しICカード（スマートカードという）のデータのリード/ライトを行う。MS制御回路61は、MS（磁気ストライプ）リーダー31の制御を行う。LCD制御回路62は、LCD（液晶ディスプレイ）32-1の表示制御を行う。マトリクスKB制御回路63は、テンキー32-2の入力を認識する。メモリコントローラ64は、ボード7上の各種メモリ（ROM65、SRAM66、FLASH67、SDRAM68）との入出力制御を行う。シリアルポート69～72は、シリアルデータの入出力を行うため、ボード7のドライバ73～75に接続される。これらは、いずれもCPUバス4-2に接続される。

【0056】

図8は、決済用LSIが搭載された電子装置のシステム構成図であり、POSシステムを示している。ネットワーク35に、ストアコントローラ20と、複数のPOS10が接続されている。POS10には、ICカードリーダー/ライタ30が接続されている。ストアコントローラ20と、複数のPOS10とには、前述の決済用LSI（IFDという）2が設けられ、決済データを直接やりとりする。

【0057】

顧客のICカード34-1は、IFD2を介しPOS用ICカード34-2と交信し、POS用ICカード34-2は、IFD2、ターミナルコントローラ11、ネットワーク35、ターミナルコントローラ11、IFD2を介しストアコントローラ20のICカード34-2と交信する。

【0058】

例えば、ICカードで電子決済を行う場合には、顧客のICカード34-1の

データは、I F D 2 を介し P O S 用 I C カード 3 4 - 2 に格納される。その後、P O S 用 I C カード 3 4 - 2 の格納データは、I F D 2、ターミナルコントローラ 1 1、ネットワーク 3 5、ターミナルコントローラ 1 1、I F D 2 を介しストアコントローラ 2 0 の I C カード 3 4 - 2 に格納される。

【 0 0 5 9 】

このシステムでは、I F D 2 により、電子決済データのルートがクローズしているため、決済データ（パスワード、口座番号、残高等）が漏れるおそれがないため、安全性が高い。

【 0 0 6 0 】

しかし、前述のように、デバッグ I / F を利用して、C P U 2 - 2 にアクセスすれば、決済データ（パスワード、口座番号、残高等）を不正取得でき、悪用されるおそれがある。従って、本発明の認証機構は、このような用途に特に有効である。

【 0 0 6 1 】

〔他の実施の形態〕

上述の実施の態様の他に、本発明は、次のような変形が可能である。

（１）前述の実施の形態では、認証により、リセット信号を解除しているが、デバッグ I / F 2 - 1 のクロック入力側に、ゲートを設け、認証により、クロック入力を許可するようにしても良い。

（２）前述の実施の形態では、一致判定後、タイマーで時間待ちしたが、一致判定前に、タイマーで判定の時間待ちをおこなうこともできる。

（３）一致判定により、不一致を検出した場合には、これを周辺回路に通知すると良い。これにより、周辺回路は、不正アクセスと判定し、例えば、セキュリティの必要なデータを消去する等の処置をとることができる。

（４）システム L S I をカード決済用で説明したが、他の用途のものに用いても良い。

（５）C P U のデバッグ I / F で説明したが、他の回路のデバッグ I / F に適用できる。

【 0 0 6 2 】

以上、本発明を実施の形態により説明したが、本発明の主旨の範囲内で種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【 0 0 6 3 】

(付記)

(付記 1) 内部回路と、外部から前記内部回路をデバッグするためのデバッグ I / F 回路と、前記デバッグ I / F 回路とデバッグ端子との間に設けられ、前記デバッグ I / F 回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と前記送信鍵とから認証を行い、前記デバッグ I / F 回路の動作を許可する認証回路とを有することを特徴とする L S I。

【 0 0 6 4 】

(付記 2) 前記認証回路は、前記動作の許可のため、前記デバッグ I / F 回路へのリセット信号を解除することを特徴とする付記 1 の L S I。

【 0 0 6 5 】

(付記 3) 前記認証回路は、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合することを特徴とする付記 1 の L S I。

【 0 0 6 6 】

(付記 4) 前記認証回路は、前記動作許可の時間待ちを行うことを特徴とする付記 1 の L S I。

【 0 0 6 7 】

(付記 5) 前記認証回路は、前記送信鍵を乱数により生成することを特徴とする付記 1 の L S I。

【 0 0 6 8 】

(付記 6) 内部回路と、外部から前記内部回路をデバッグするためのデバッグ I / F 回路と、前記デバッグ I / F 回路とデバッグ端子との間に設けられ、前記デバッグ I / F 回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグ I / F 回路の動作を許可する認証回路とを有する L S I を搭載したことを特徴とする電子装置。

【 0 0 6 9 】

(付記 7) 前記認証回路は、前記動作の許可のため、前記デバッグ I / F 回路へのリセット信号を解除することを特徴とする付記 6 の電子装置。

【 0 0 7 0 】

(付記 8) 前記認証回路は、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合することを特徴とする付記 6 の電子装置。

【 0 0 7 1 】

(付記 9) 前記認証回路は、前記動作許可の時間待ちを行うことを特徴とする付記 6 の電子装置。

【 0 0 7 2 】

(付記 1 0) 前記認証回路は、前記送信鍵を乱数により生成することを特徴とする付記 6 の電子装置。

【 0 0 7 3 】

(付記 1 1) デバッグ I / F 回路を利用して、外部から内部回路をデバッグするデバッグ方法において、前記デバッグ I / F 回路の起動時に、前記外部に送信鍵を送信するステップと、前記外部から受信した信号と前記送信鍵とから認証を行い、前記デバッグ I / F 回路の動作を許可するステップとを有することを特徴とするデバッグ方法。

【 0 0 7 4 】

(付記 1 2) 前記認証ステップは、前記動作の許可のため、前記デバッグ I / F 回路へのリセット信号を解除するステップを有することを特徴とする付記 1 1 のデバッグ方法。

【 0 0 7 5 】

(付記 1 3) 前記認証ステップは、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合するステップを有することを特徴とする付記 1 1 のデバッグ方法。

【 0 0 7 6 】

(付記 1 4) 前記認証ステップは、前記動作許可の時間待ちを行うステップを有することを特徴とする付記 1 1 のデバッグ方法。

【0077】

(付記15) 前記送信ステップは、前記送信鍵を乱数により生成するステップを有することを特徴とする付記11のデバッグ方法。

【0078】

(付記16) デバッグ装置と前記デバッグI/F回路の間に設けられた識別装置が、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信するステップを、更に有することを特徴とする付記11のデバッグ方法。

【0079】

(付記17) 内部回路と、外部から前記内部回路をデバッグするためのデバッグI/F回路と、前記デバッグI/F回路とデバッグ端子との間に設けられ、前記デバッグI/F回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグI/F回路の動作を許可する認証回路とを有するLSIをデバッグするデバッグ装置であって、デバッグユニットと前記デバッグI/F回路の間に設けられ、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信する識別装置を有することを特徴とするデバッグ装置。

【0080】

【発明の効果】

以上説明したように、本発明によれば、次の効果を奏する。

【0081】

デバッグI/F回路とデバッグ端子の間に認証回路を設けたため、第3者のデバッグI/Fを利用して、内部回路の動きをリバースエンジニアリングする等の不正行為から内部回路を守る事ができ、従来の装置よりもより高いセキュリティを保つ事ができる。

【0082】

又、識別装置3とLSI2とのセットでセキュリティを実現するため、物理的接続と認証アルゴリズムにより、セキュリティを行うため、高いセキュリティが可能となる。また、PC5による不正解析も困難である。

【図面の簡単な説明】

【図 1】

本発明の一実施の形態の L S I のブロック図である。

【図 2】

図 1 の認証処理の説明図である。

【図 3】

図 1 の L S I のデバッグ方法の説明図である。

【図 4】

図 1 の L S I の不正アクセス防止の説明図である。

【図 5】

図 1 の他の認証処理の説明図である。

【図 6】

図 1 の L S I を搭載した電子装置の説明図である。

【図 7】

図 1 の周辺回路のブロック図である。

【図 8】

図 6 の L S I を搭載した P O S システムの構成図である。

【図 9】

従来技術の説明図である。

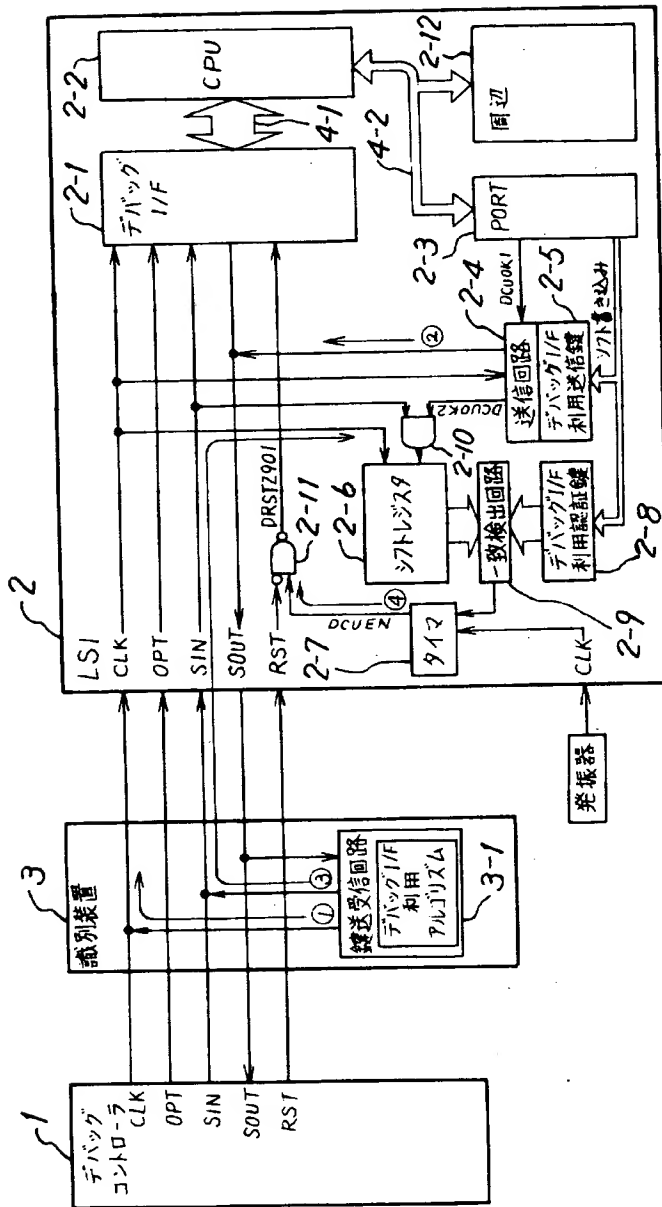
【符号の説明】

- 1 デバッグコントローラ
- 2 L S I
- 3 識別装置
- 2 - 1 デバッグ I / F 回路
- 2 - 2 C P U
- 2 - 3 ~ 2 - 1 1 認証回路
- 2 - 1 2 周辺回路

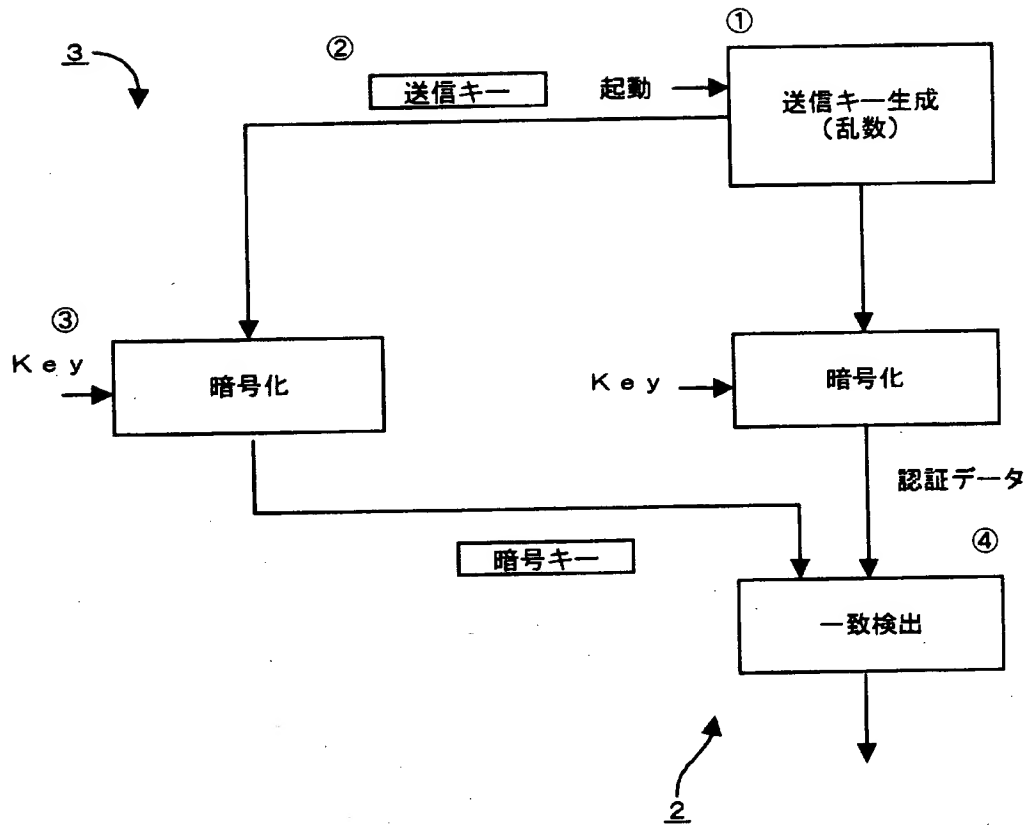
【書類名】

図面

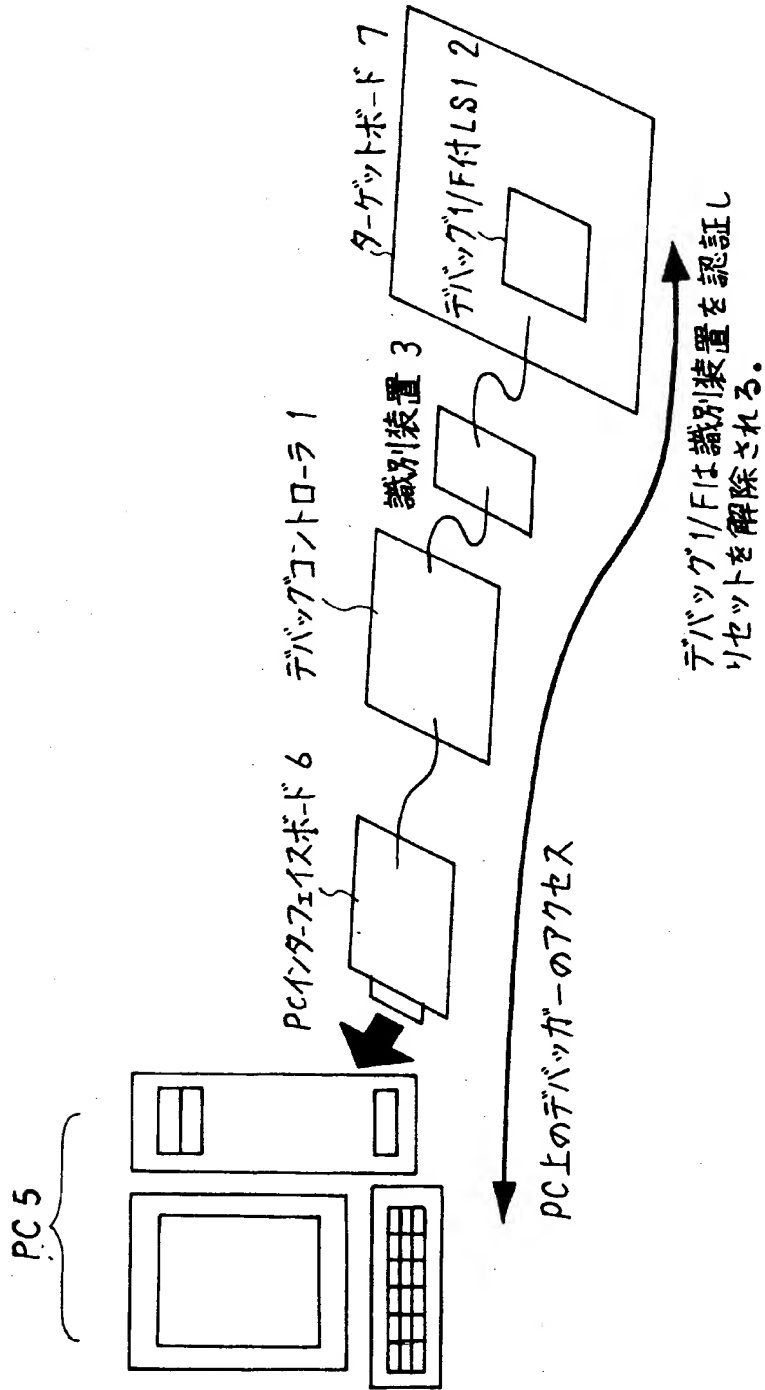
【図 1】



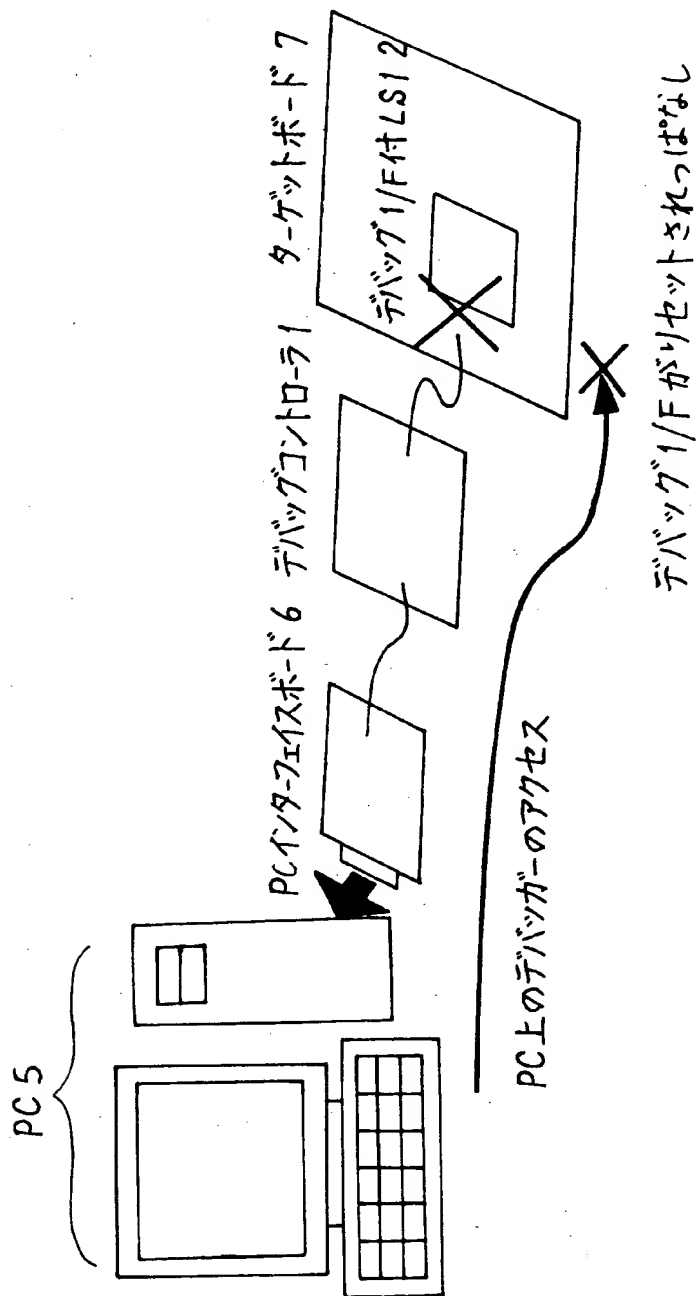
【図 2】



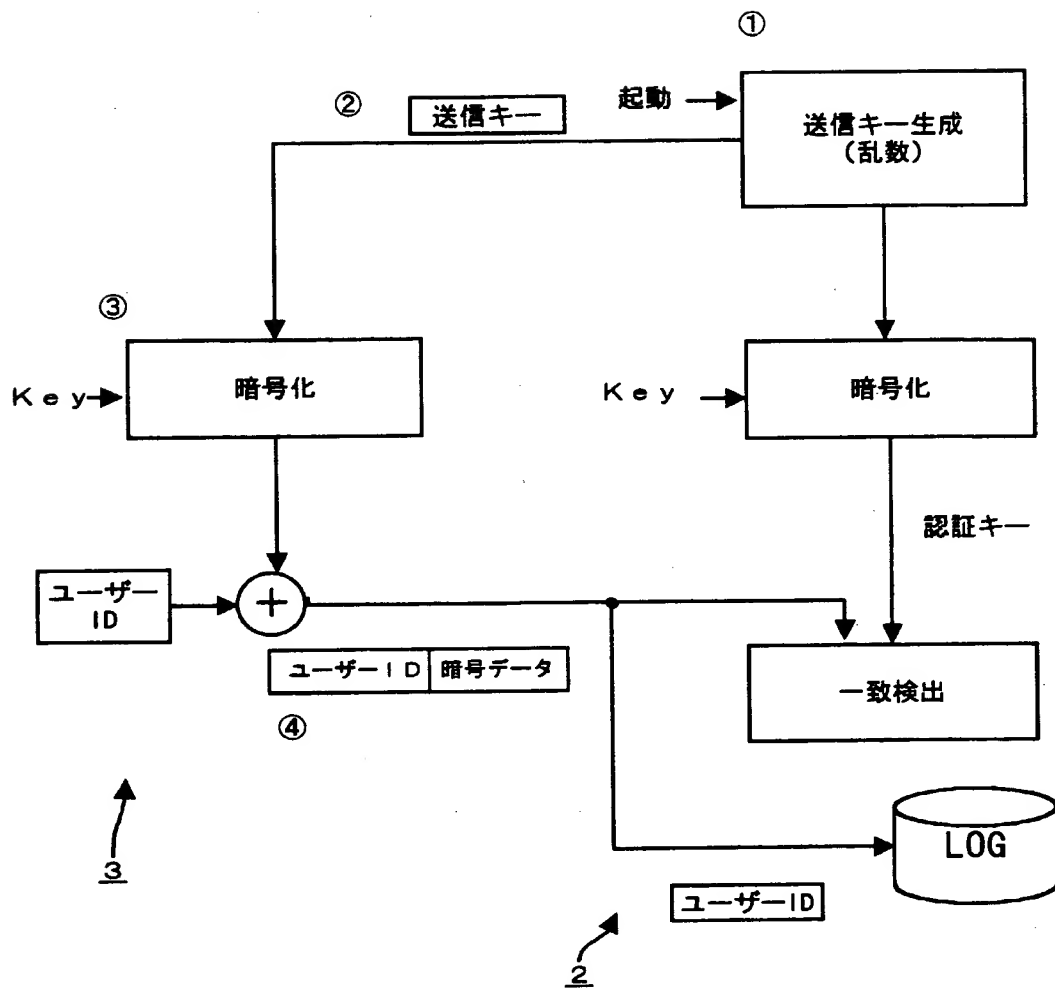
【図3】



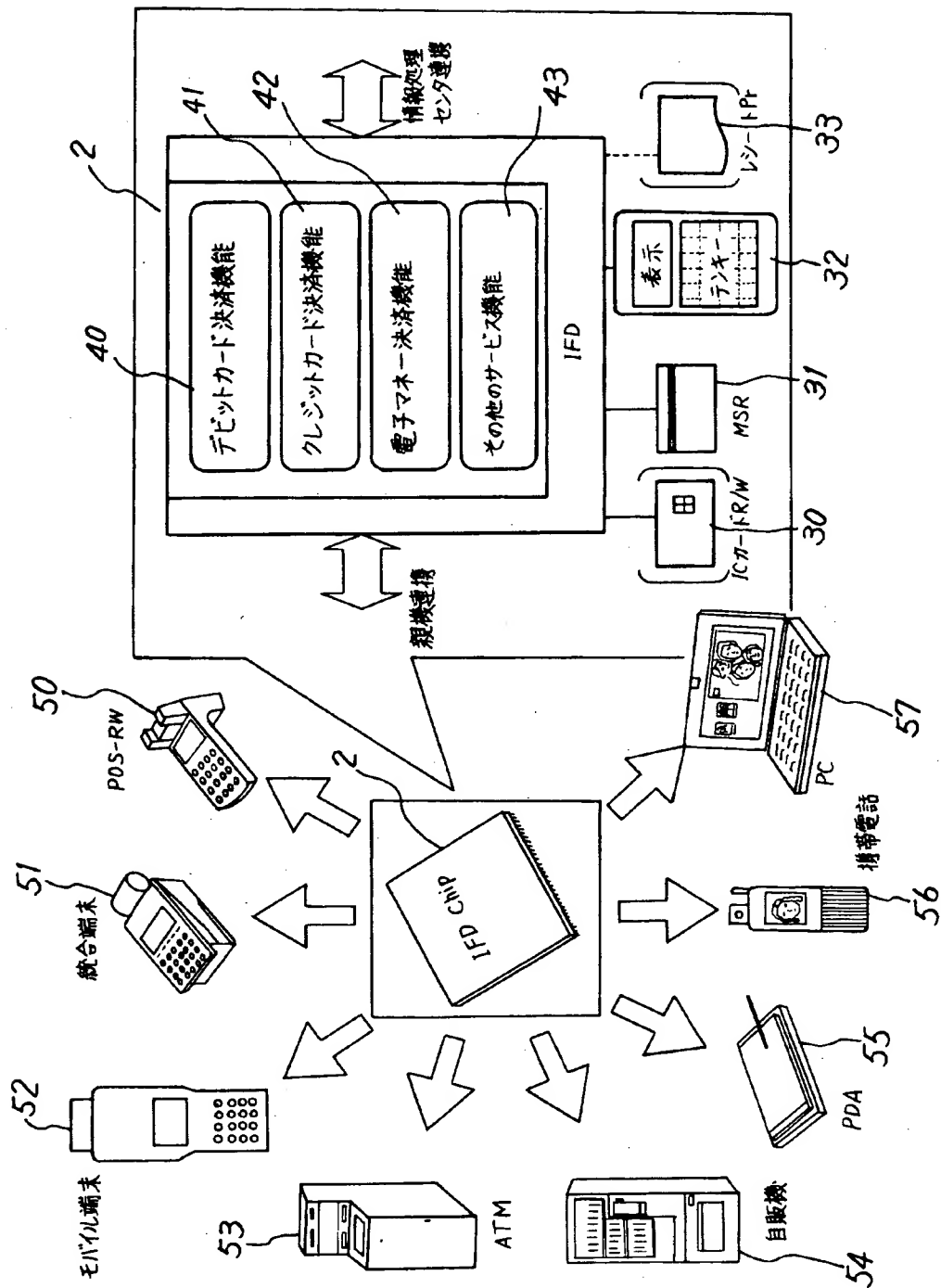
【図4】



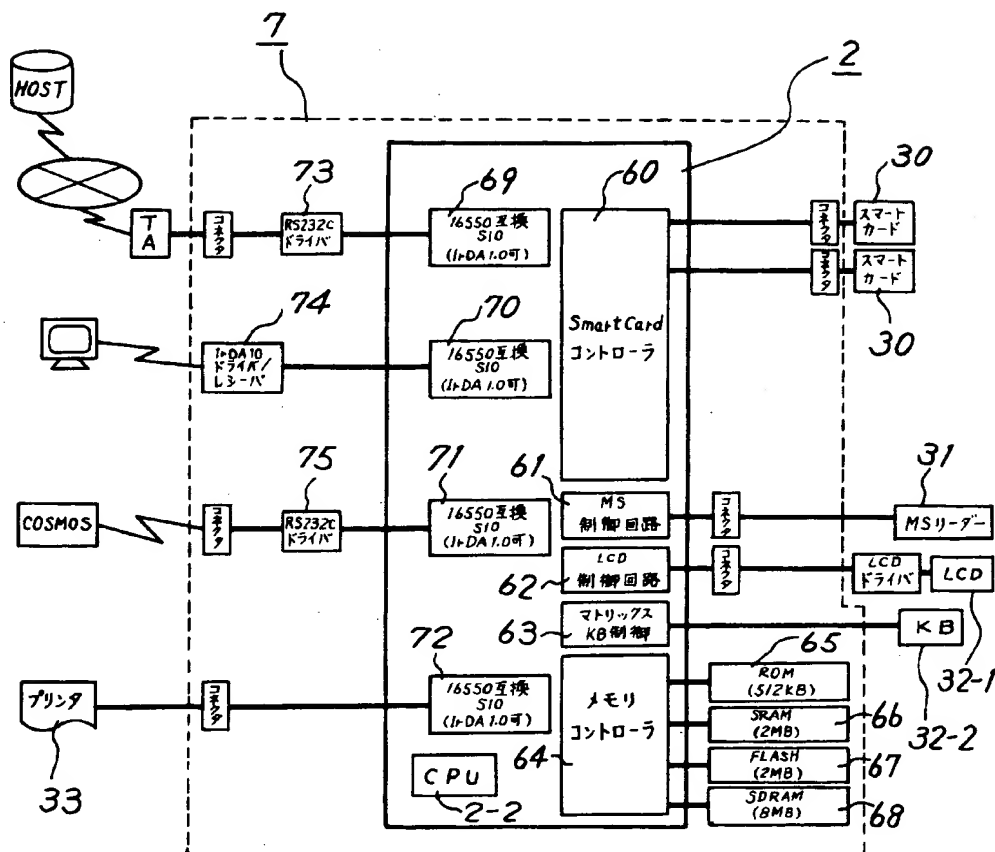
【図 5】



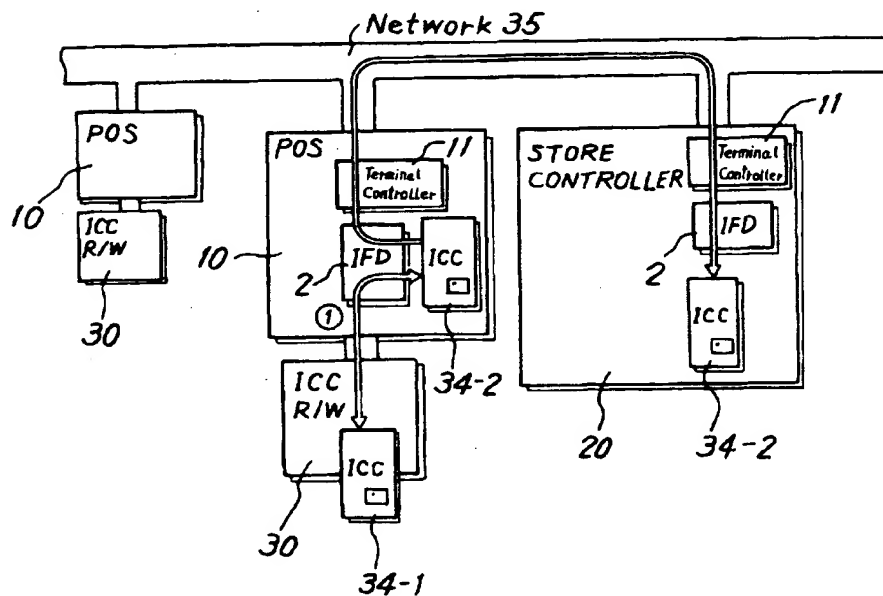
【図6】



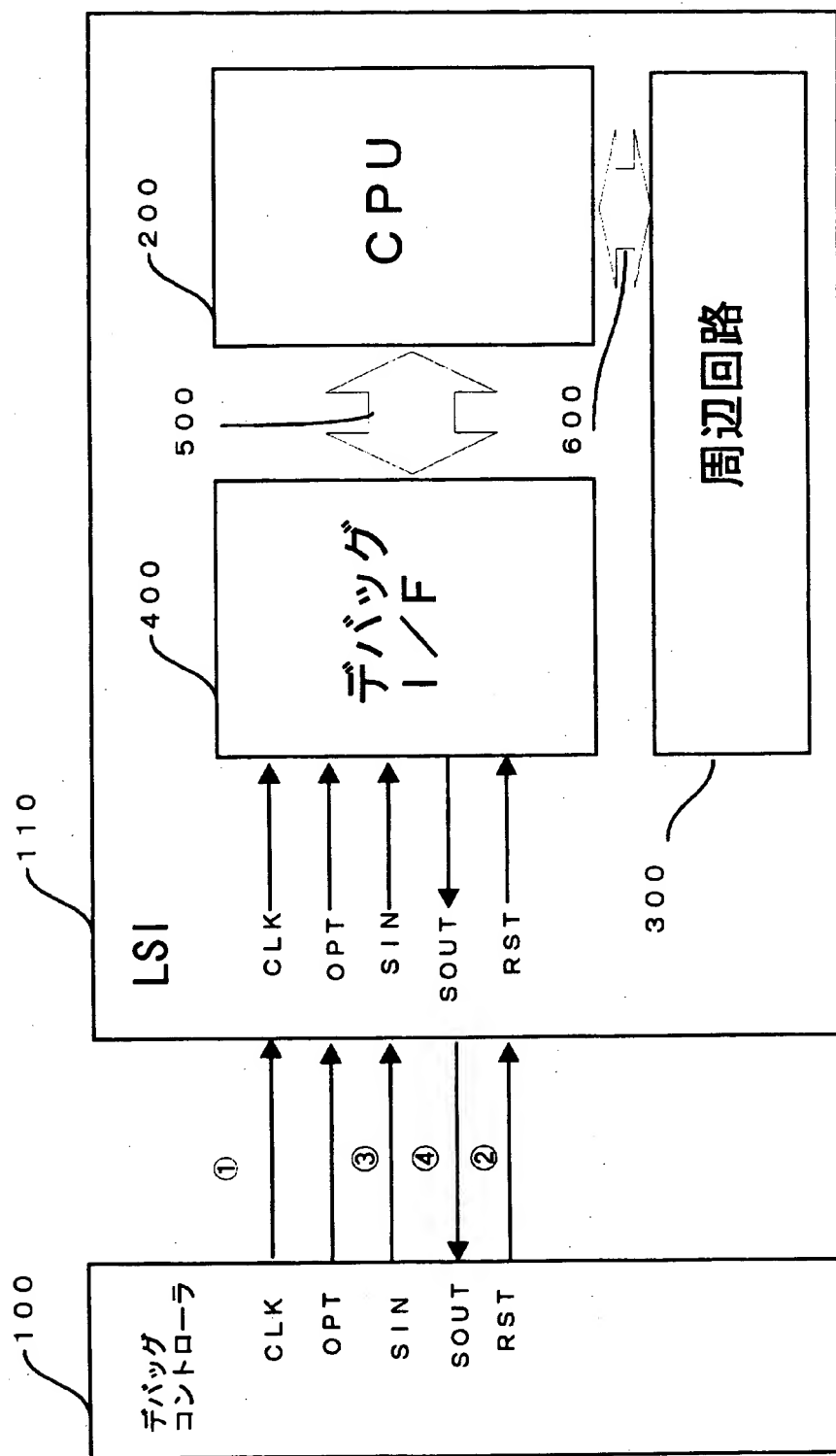
【図7】



【図8】



【図9】



【書類名】 要約書

【要約】

【課題】 システム L S I において、デバッグ I / F からの内部回路へのアクセスを制限する。

【解決手段】 デバッグ I / F 回路 (2 - 1) とデバッグ端子の間に、認証回路 (2 - 3 ~ 2 - 1 1) を設ける。認証回路は、起動時に、外部に送信鍵を送信し、受信信号と送信鍵から認証を行い、デバッグ I / F へのアクセスを許可する。認証回路により、デバッグ I / F からの第 3 者の不正アクセスを防止できる。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2000-199266
受付番号	50000824385
書類名	特許願
担当官	高田 良彦 2319
作成日	平成 12 年 7 月 7 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
【氏名又は名称】	富士通株式会社

【代理人】

申請人

【識別番号】	100094514
【住所又は居所】	神奈川県横浜市港北区新横浜 3-9-5 第三東 昇ビル 3 階 林・土井 国際特許事務所
【氏名又は名称】	林 恒徳

【代理人】

【識別番号】	100094525
【住所又は居所】	神奈川県横浜市港北区新横浜 3-9-5 第三東 昇ビル 3 階 林・土井 国際特許事務所
【氏名又は名称】	土井 健二

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社